

Process Model for Defining Space Sensing and Situational Awareness Requirements

Gregory Orndorff

Senior Professional Staff, Johns Hopkins University
Applied Physics Laboratory
Laurel, MD 20723-6099
USA

greg.orndorff@jhuapl.edu

ABSTRACT

A process model for defining systems for space sensing and space situational awareness is presented. The paper concentrates on eight steps for determining the requirements to include: decision maker needs, system requirements, exploitation methods and vulnerabilities, critical capabilities, and identify attack scenarios. Utilization of the USAF anti-tamper (AT) implementation process as a process model departure point for the space sensing and situational awareness (SSSA) mission area is presented. The AT implementation process model, as an accepted process application pertains directly to the analysis of military space system sensing requirements. In the paper a new process model is presented with generic SSSA examples and questions for each process step leading to preliminary environmental requirements. The resulting SSSA requirements analysis model allows government program managers and acquisition officials to trade cost, schedule and technical performance of identified SSSA solutions against the identified vulnerabilities and allocates the solution set between spacecraft, ground system, or other sensing architectures. The model allows the requirements analyst to frame sensing solutions against the attack scenarios such that decision makers can weigh cost versus benefit to protecting the critical space capability. The resulting model provides for a common lexicon and taxonomy for requirements discussion between NATO members. The paper also introduces the temporal quality to the SSSA needs based on the constant march of technology by introducing a concept for updating the SSSA requirements analysis based on the periodicity of Moore's law.

1.0 ACKNOWLEDGEMENTS

Special thanks to Dr. Yolanda King from the Air Force Research Laboratory, USA for her support and encouragement and to two of my contemporaries at JHU/APL for their collaboration and review of this paper: Dr. Dan McMorro and Dr. Pete Tennyson.

2.0 BACKGROUND

“You can see a lot just by observing” Yogi Berra

All strategic and tactical action necessitates environmental awareness and context of the situation. Therefore, any action or decision involving space-based assets (or capabilities that can affect space-based assets) must rely on knowledge of that special environment generally known as ‘space’. Space in a vain similar to

Orndorff, G. (2006) Process Model for Defining Space Sensing and Situational Awareness Requirements. In *Space Sensing and Situational Awareness* (pp. 4-1 – 4-10). Meeting Proceedings RTO-MP-SET-105, Paper 4. Neuilly-sur-Seine, France: RTO.
Available from: <http://www.rto.nato.int/abstracts.asp>.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 01 APR 2006		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Process Model for Defining Space Sensing and Situational Awareness Requirements (U)				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Senior Professional Staff, Johns Hopkins University Applied Physics Laboratory Laurel, MD 20723-6099 USA				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES See also ADM401234. RTO-MP-SET-105, presented at the RTO Sensors and Electronics Technology Panel (SET) Specialist Meeting held at the Maui High Performance Computing Center (MHPCC), Maui, Hawaii, USA, 24-25 April 2006., The original document contains color images.					
14. ABSTRACT See the report.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 10	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified - NATO	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Process Model for Defining Space Sensing and Situational Awareness Requirements

terrestrial sensing has a multitude of modalities, issues, and phenomenology. Space however, is tremendously more vast, difficult to operate in, and expensive to exploit. Because space systems play an important role for NATO forces deployed around the world there is an interest in improving the operational understanding of the space domain. Space Sensing and Situational Awareness (SSSA) together provide the capability to understand the domain and present the operational understanding to decision makers. Obtaining requirements for SSSA systems can be an arduous task. A process model utilizing a disciplined approach could significantly improve the efficiency of the system engineer in gathering SSSA requirements and also provide NATO decision makers with a tool and lexicon to develop an operational picture of space assets and their utility to NATO forces.

3.0 THE ANTI-TAMPER MODEL

Preference for reuse or to leverage previous work often provides an efficiency not found when creating from whole cloth. Likewise, when identifying a requirements process for SSSA the author utilized a tool from earlier work by others – the USAF Anti-Tamper implementation process. Like any competent technology enterprise, the Air Force desires to preserve their investment in technological advantage and specifically has concerns with others reverse engineering their fielded capabilities¹. In fact, United States Public Law and Policy drives DoD to protect critical information and technology. One output of their efforts is an anti-tamper (AT) implementation process shown in Figure 1 (replicated from AFRL/SPI pamphlet). The process as summarized in the graphic has several features applicable to SSSA requirements definition. There are two major attributes that the proposed process model will borrow. First, the comparison of current capabilities to prospective future ones that allows the decision maker to discern the value added – in other words, is the cost, schedule, and risk worth the increase in capability. The second is to characterize the perceived threats and vulnerabilities which also provides insight into the cost or risk of inaction. These major attributes as well as several secondary ones will be seen in the SSSA model that follows.

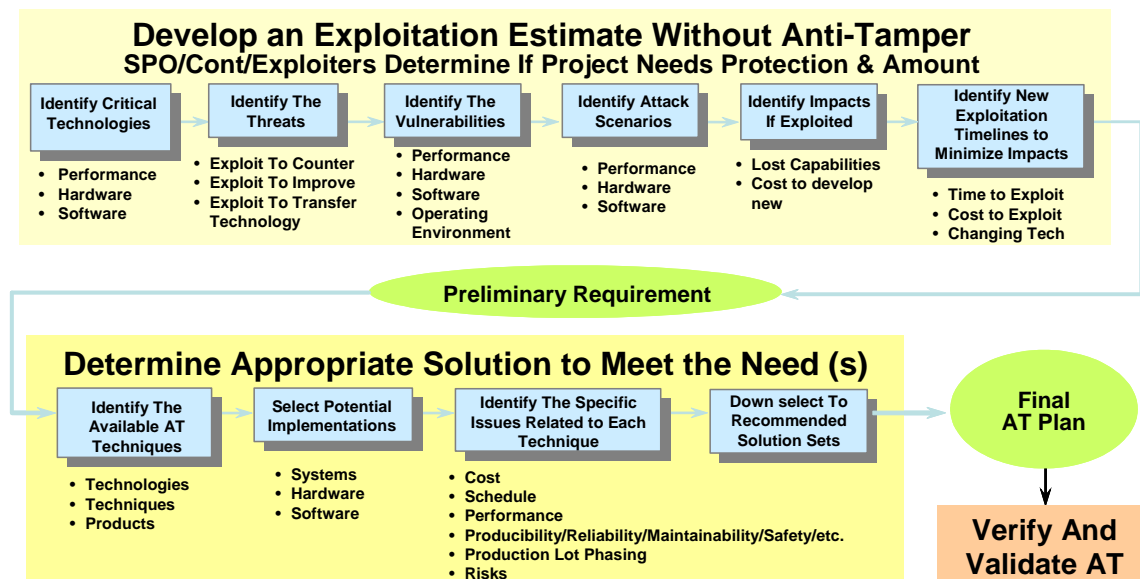


Figure 1: Anti-Tamper Implementation Process

¹ U.S. Under Secretary of Defense for Acquisition and Technology letter dated 4 February 1999, Titled: Implementation of Anti-Tamper (AT) Techniques in Acquisition Programs signed by Mr. J. S. Gansler

A notable feature of the AT process is the stepwise assessment of the environment (the six process steps in the top block) to derive a preliminary requirement that includes deliberate threat assessments.

4.0 CHARACTERIZING THE ENVIRONMENT

The goal of this paper is to socialize a process model for collecting SSSA requirements. Applying a disciplined approach to collecting requirements should ensure the appropriate solution set is considered. A suggested process model for developing SSSA solutions is shown Figure 2. The top segment of eight process steps represents the gathering of the driving requirements. The order of the eight process steps while not notional does enjoy flexibility in their order and degree of parallelism. The reader should not assume the model requires the steps to be accomplished in order or in series. Another note, the model is not specific to NATO requirements but is rather put forth a generic tool albeit focused on SSSA. Following are explanatory sections for each process step leading to the “Preliminary Requirements” stage (represented by the green oval in the figure). At this stage, all the relevant driving requirements should be known and proceeding to the mission requirements and solution part of the model can commence. This paper will not further define the process steps required to obtain a solution set. This part of the process model is shown in the graphic for the sake of completeness. Subsequently, a detailed description is left as a follow-up effort by the author or others.

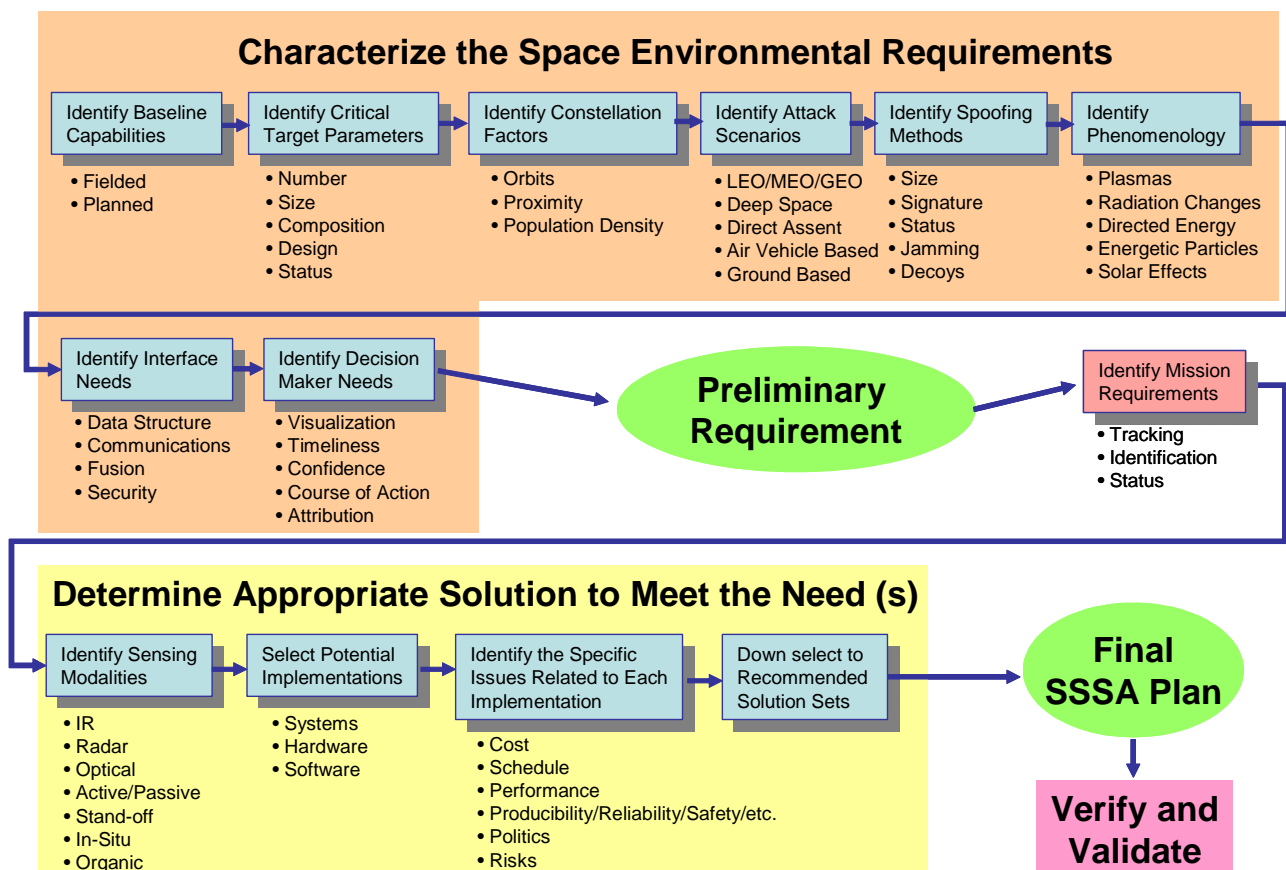


Figure 2: Process Model for Developing SSSA Solutions

Process Model for Defining Space Sensing and Situational Awareness Requirements

The eight separate requirement gathering steps that lead to establishing a preliminary set of requirements provides the systems engineer with an ordered process for determining the driving requirements. Within each step are elements that will be presented as questions and can be thought of as a checklist approach to defining the environmental attributes. Prioritizing the requirements according to the intended mission of the fielded solution is not presented but the author recognizes that solutions can be segmented into mission areas such as: tracking, conjunction avoidance, identification, imaging, interrogation, and determining status. Future missions that SSSA systems may support could also include: raising/lowering orbits, de-orbiting objects, collection, status changing and system upgrades. Different mission solutions will drive the different priority assessments of the requirements. For instance, the tracking mission solution set is not driven by the target parameter of design like a mission to upgrade systems on orbit would be. Before proceeding from the environmental requirements to determining the SSSA solution, the mission requirements must be defined.

A benefit of a standardized process model is the common lexicon that the NATO community uses in discussing the SSSA requirements, missions, and solutions - hence, another reason to discuss and adopt a methodology. The eight process steps are defined as, and will subsequently be presented: 1. Identify baseline capabilities. 2. Identify critical target parameters. 3. Identify constellation factors. 4. Identify attack scenarios. 5. Identify spoofing methods. 6. Identify phenomenology. 7. Identify interface needs. 8. Identify decision maker needs.

4.1 Step 1: Identify Baseline Capabilities

Understanding the fielded and planned (near-term systems that are funded and therefore enjoy confidence in being fielded) is the first step in the SSSA process model. The capabilities of the fielded systems are not strictly speaking an environmental factor and this step could be performed during the solution implantation phase. Questions for this step include but are not limited to:

- What are the current fielded SSSA sensors, systems, and processes?
- What sensors, systems, and processes are planned and what are their respective operational start dates?
- Further define each one by ownership, lifecycle, data product, operating system, operating cost, and limitations.
- What open source information is available (relevant during steps 4 and 5)?

4.2 Step 2: Identify Critical Target Parameters

The targets that need to be sensed, tracked, and characterized must first be described in sufficient detail to ensure sensors and systems can characterize them. Their status, number and size (e.g. radar cross section) are driving requirements and also need to be forecast for into the future. Since space sensors have a timeline associated with fielding operational capabilities the future state must be assumed. How many more objects will be in orbit? Will they be smaller or larger? How many active systems will be inactive in the near-future? At this step assumptions are not made regarding mission requirements. Instead, capturing the current and near-future space object characteristics is the intent. Additional parameters include external composition of the space objects as they pertain to reflectance, emissivity, etc. Design details in the form of a database may be a requirement.

4.3 Step 3: Identify Constellation Factors

The next step is to build environmental understanding of the space object population density. What orbits are utilized now and in the future? How many objects are in each orbit? How are the spaced? How often are

they moved? Since a model or simulation may be needed, care in collecting these environmental requirements is needed to ensure sufficient information is known to correctly model the space environment with minimal errors. Significant earlier work in this area has been accomplished and is available commercially.

4.4 Step 4: Identify Attack Scenarios

Identifying threats is an important step in understanding the environment for SSSA. During the requirements process a “Red Force” team that is separate for the systems engineering effort could be used to identify attack scenarios. These scenarios should encompass the spectrum of techniques and technologies available in the open market to the adversary. After an exhaustive array of scenarios is assembled they should be characterized by their impact on NATO systems and their probability of occurrence. This weighting is similar in process to commonly used relative risk weighting systems. The product of the impact and probability produces a scale factor that enables the attack scenarios to be ranked.

$$\begin{aligned} \text{Probability of Occurrence (Po)} \times \text{Probability of Success (Ps)} \times \text{Impact to employed systems (Is)} \\ = \text{risk scale factor (RSF)} \end{aligned}$$

The probability of occurrence for each scenario is based on factors like: cost to employ, workforce skills or expertise, and needed equipment to design, build, or operate. The probability of success is a qualitative measure of the adversary. The impact part of the equation can be expressed in monetary terms or as a simple scalar. In either case the impact should be assessed relative to military space and ground systems, as well as international, commercial and civil systems. Attack scenarios can and should represent the broadest range of available cases. A couple of example scenarios culled from open sources include²:

- Ground attack. A ground station used for commanding a space system is attacked by terrorists using improvised explosive devices to disrupt satellite operations.
- Direct ascent attack. Direct ascent weapons could be ideal weapons for a nation state intent on destroying an orbiting target while preserving anonymity. A tactical aircraft carrying an anti-satellite rocket could take off from a non-associated 3rd country by bribing a local leader without any involvement by the nation’s government.
- Orbital attack. In this scenario, an organization launches a supposedly scientific mission to the Moon and declares an anomaly. After a certain interval, the spacecraft is reactivated and disburses multiple kill vehicles against GEO targets.

This step provides tremendous insight into NATO capability changes should infrastructure or space assets themselves become compromised.

4.5 Step 5: Identify Spoofing Methods

Consideration should be given to the ability of space systems to be designed to counter detection. Methods could include passive and active measures. Space objects that are deliberately made as small as possible could also be design to have a substantially reduced radar signature and include surface coatings to reduce reflectance and emissivity. Anticipated jamming and decoy deployment capabilities may lead to requirements to characterize emissions and or produce automated alerts for deployments. These target requirements are captured separately from step 2 as they should be classified at a higher level than the other environmental

² Unclassified sources like a recent article in *Armed Forces Journal* by Frank Hoffman

Process Model for Defining Space Sensing and Situational Awareness Requirements

requirements. One method to capture these requirements is to leverage the red force team suggested in the previous step. Questions include:

- What coatings are available to reduce signatures?
- What active methods are available to spoof sensing systems?
- How can the different sensing modalities be spoofed?
- What methods could be employed to enable an active space object to appear inactive?

Results from this step may identify requirements for countering the spoofing methods. Like the attack scenario step, these requirements may need a separate security classification within the SSSA requirements family.

4.6 Step 6: Identify Phenomenology

Space weather is an important environmental factor. In addition, environmental conditions will need active monitoring or sensing to correctly understand the space environment in real-time. The spectrum of space weather attributes should be assessed in this step. Major phenomenologies that may require active sensing to support space situational awareness include: local plasmas, changes in radiation environment, directed energy, energetic particles, solar effects, micro-meteoroids, etc. One reason this step follows the previous attack and spoofing steps is for the situation where the selected threat cases drive a requirement for space environmental sensing not associated with the threat object itself. Space weather phenomena will not uniformly affect threat scenarios in the same manner.

4.7 Step 7: Identify Interface Needs

This step provides for gathering requirements related to data and networks. Not specifically called out in the process model is training which could also be captured in this step. Security is a requirements driver that is briefly covered.

Data structures are often overlooked in the requirements process. Interfacing with currently fielded systems may not allow significant modification of data streams and hence drive flexibility into a solution design. A common data structure with meta-tagging should be assessed as a requirement for SSSA systems. Communications between sensors, platforms, systems, and ground facilities is a broad class of requirements also assessed in this step. Communications between NATO systems and between external systems and NATO systems should be reviewed for driving requirements (for instance bandwidth limitations) that impact SSSA systems.

Ultimately the SSSA system is attempting to provide knowledge from a disparate set of sensors and databases. Fusion algorithms will be required to digest the data and produce situational awareness of the space domain. Different levels of fusion may be necessary in different parts of the SSSA infrastructure to service the number of system operators available or desired. Hence there is a strong correlation between the fusion levels attainable and the recurring cost to employ SSSA systems. Identifying the levels of fusion required in a system may lead to additional requirements on sensors, data structures, operating systems, etc.

Security will always generate requirements and SSSA for NATO will be no exception. Physical security of ground installations is but one aspect of the security requirements SSSA will identify. Multi-level security will have to be addressed as parts of fielded, planned, or recommended capabilities may have different security requirements. A major driver will be those external data sources that carry their own security

requirements. All the different NATO security needs and requirements are collected in this step but not otherwise described in this paper.

4.8 Step 8: Identify Decision Maker Needs

The last step in the series to capture the SSSA requirements is to understand the needs of the data operator and decision maker (also referred to as the knowledge worker). Before describing this step let me reiterate that the steps described in the model are not established as a series and this step to determine the requirements of the knowledge worker is a notable example. This step could easily be the first in the series. The logic used to make it the last step in gathering requirements is that there could be insights or issues discovered in the earlier steps that lead the knowledge worker or the requirements gatherer to identify needs that may not have been discovered if this step were the first in the series.

The knowledge worker for SSSA will have several needs and requirements. The initial consideration is the education and training level of those workers as it will range from specially trained and focused non-commissioned officers to high ranking senior officers that may not have the speciality training (on space weather or orbital mechanics for instance). The major areas within this step to be addressed include: Visualization, Timeliness, Confidence, Courses of Action, and Attribution. Attribution being perhaps the most stressing requirement of all.

Space situational awareness has unique attributes when compared to operational pictures of the ground or air environments. Creating a visualization method for the space domain should be able to leverage some features of ground and air operational pictures. For instance showing status of ground installations that control space assets is a simple one. Understanding that there are over 10,000 objects in space and that the one having the most impact on a given situation may be on the opposite side of the planet from the operational view presents some challenges. Clearly operational views will need to be modified by the operator or decision maker depending on their responsibility or position. Standardization will be necessary and at the same time allow customization. Cognitive engineering efforts should help in identifying system requirements for space situational awareness.

System requirements related to timely processing of sensor data represent one end of the range of this subset of requirements. The other end can be represented as forecasting space object position into the future with sufficient accuracy to predict conjunctions when propulsion events occur. A timeliness requirement may be a derived one from a whole host of awareness metrics from database algorithms necessary to provide situational awareness to system processes associated with SSSA systems. Timeliness requirements may drive constellation sizes and hence be a major cost driver that should be assessed against relative value added. A series of questions that could be used during the requirements process could include:

- How often does the event occur?
- How quickly does the process have to occur to keep data relevant?
- When do other parts of the system have to be notified or associated?
- Can forecasting future states be beneficial?
- Is accuracy associated with timeliness?
- Does phased reporting (incremental status changes versus reporting an end state when a high confidence is known) provide benefit?

Process Model for Defining Space Sensing and Situational Awareness Requirements

The last question provides a link to the next set of questions.

SSSA confidence levels will need to be defined to provide decision makers sufficient information to take action. Errors will occur across every level of a complex system. Errors will propagate through a system and have to be characterized for the decision maker using the system. Confidence levels will drive a requirement to sufficiently characterize the accuracy of sensor data about an event, the accuracy of database algorithms, the accuracy of predicted events, and the accuracy of courses of action to mitigate predicted events. These different confidence levels need summarization for display in an operational context. Several questions attempt to capture these requirements:

- What confidence level is needed to take action?
- What is the impact of a decision error?
- Does the confidence level change dependent on the action effects or assets used?
- What confidence level should be used to report anomalies?
- How confidence levels be should communicated (scalar, percent, color)?
- Should different confidence levels be used in different parts of SSSA systems?

Once an anomaly or status change or threat occurs, the SSSA system will be required to support the formulation of available courses of action (COAs). To produce COAs, the SSSA system will need the capability to run simulation algorithms to order to safely employ space assets. COAs involving ground assets should be a more simple case. The exploitation of the situational awareness will require the same databases to be utilized to identify viable COAs. The COAs will need to be automatically ranked and associated with a confidence level in order to be presented to the system operator. Depending on the decision process used, there may be other requirements levied on the COA generating element of the SSSA system. For instance, when the need occurs to produce COAs, they may need to be known at several layers of an organization or to external stake holders even, all at the same time and in such a fashion to allow collaboration in real time. Certain COAs may require senior decision makers while the other end of the scale may allow simple actions to be the operational norm and occur on a routine basis. A hierarchy and standards will be necessary for utilization of COAs within the SSSA system.

The ability of the SSSA system to enable attribution of anomalies may introduce a unique set of requirements. After an event or anomaly occurs, system users will need to ascertain who or what is responsible. If space weather and an on-board spacecraft anomaly are discounted, the need to determine attribution of an event to a terrestrial entity may be a significant requirement. Even this first level of attribution (internal versus external to the spacecraft) may be indeterminate. It may not be possible to determine with a significant confidence level that the effect was caused by a space or ground asset. If the SSSA system is constrained, a set of possible attribution entities may have to be handed off to an external organization for further characterization and investigation. Attribution in the space environment is a difficult task since physical forensics is nearly impossible. The attribution requirement may lead to an expansion of SSSA databases or linking to intelligence data. The requirements levied by the decision makers who utilize the SSSA systems may produce the driving requirements for the system.

5.0 PRELIMINARY REQUIREMENT

The end product of the eight steps is a set of space environmental requirements along with threat scenarios and space weather phenomenology. Sufficient information is available at this step in the process model to

understand the current and future states that SSSA systems need to or will need to operate in. The operational understanding that space situational awareness needs to support is also known at the end of the recommended requirements process. At this juncture, modelling and simulation effort could be undertaken to provide an environment to do mission analysis and investigate the trades between solution implementations.

6.0 SOLUTION THOUGHTS

Requirement analysis while necessary is never sufficient to discovering or designing an optimal system solution. Requirements analysis alone doesn't indicate how often the requirements should be revisited, how should relative solution sets be technically assessed (separate from risk, cost, schedule, programmatic, or political) or whether sensors should be linked to reporting systems on the space assets. The thrust of this paper is on the requirements gathering process and not the mission or solution elements. A short discussion is presented on three topics: metrics, a solution for future consideration, and how often the process should be repeated.

The NATO community will need a set of metrics established to assess the relative merit of SSSA solutions. Terrestrial systems may offer insight and should be judiciously evaluated for application to the space environment. Qualitative metrics, for instance, to assess the imagery product of a space object are not standard. When one considers that video may be a highly utilized product for space sensing, a metric for gauging the utility of the video will be necessary for the analyst to communicate requirements to the sensor designer.

The space environment while vast and seemingly empty is increasing being populated by non-government entities. Space tourism is coming as evidenced by the tireless efforts of Bob Bigelow to put hotels in orbit. Should the international community consider treating space objects like common air traffic by requiring a transponder for the sole purpose of self reporting identification, position, velocity and vector, status, etc.? Indication, Friend or Foe (IFF) systems (historically also called Radar Identification and Recognition System) should be considered a relevant analogue to a future capability. In time, a space traffic control system will be needed.

How often should NATO consider embarking on a comprehensive effort to verify needs and requirements for SSSA? Certainly some periodicity is needed. Accelerating change in technology drives the capabilities we see in space systems and our ability to sense the space environment. And let us not forget that the continual march of technology also works against us in the form of advanced capabilities for advisories or lowering the cost barrier of entry into the space domain for terrorists. Moore's law states that the number of transistors on a chip doubles about every two years. This observation about silicon integration provides a window into the worldwide technology revolution. A factor of two increase in capability every two years provides a useful milestone for identifying the periodicity of requirements analysis. The author proposes that any large system, and in this case SSSA systems in particular, have to be assessed against the near term technological capability. Situational awareness in order to be effective must provide for sensing new environments brought into existence because of technology advances. Revisiting SSSA requirements and performing a gap analysis against new threats and targets should occur every two years. Relying on the ability to forecast technology does not suffice for revisiting the requirements domain.

7.0 CONCLUSION

The proposed process model provides for a comparison of current capabilities to prospective future ones that allows the decision maker to discern the value added – in other words, is the cost, schedule, and risk worth the

Process Model for Defining Space Sensing and Situational Awareness Requirements

increase in capability. Additionally, the model forces the characterization of threats and vulnerabilities which can reveal unique requirements but also provides insight into the cost or risk of inaction. The process model provides a series of questions and issues that the requirements analyst can use to gather the requirements an SSSA system has to consider. Special requirements related to attribution, periodic assessments of the requirements and the benefit of a common lexicon are secondary issues resulting from the requirements analysis process proposed. NATO has a unique opportunity to provide value added in the space sensing and space situational awareness mission area. In order for NATO to determine appropriate capabilities to employ for space sensing and space situational awareness, an exhaustive analysis of the requirements is required. The proposed process model described is one instantiation of a methodology that could be utilized to this end.